# Department of Homeland Security Daily Open Source Infrastructure Report for 17 February 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

**Daily Highlights**

- The Chicago Tribune reports Exelon Nuclear has announced that radioactive tritium leaks have been found at two more nuclear power plant sites: Dresden Generating Station and Byron Nuclear Generating Station. (See item 2)
- The Associated Press reports officials at Reno−Tahoe International Airport demanded answers after new, high−tech equipment designed to keep the airport open in poor weather failed, causing five flight diversions and a ripple of delays. (See item 15)

**DHS Daily Open Source Infrastructure Report *Fast Jump***

**Production Industries:** Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
**Service Industries:** Banking and Finance; Transportation and Border Security; Postal and Shipping
**Sustenance and Health:** Agriculture; Food; Water; Public Health
**Federal and State:** Government; Emergency Services
**IT and Cyber:** Information Technology and Telecommunications; Internet Alert Dashboard
**Other:** Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVAED**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 16, Federal Energy Regulatory Commission* — **Federal Energy Regulatory Commission addresses U.S. energy market conditions near the end of 2005−2006 heating season.** On Thursday, February 16, the Federal Energy Regulatory Commission released the Winter 2005−2006 Energy Market Update. The report found that several factors appear to be influencing the U.S. natural gas markets. These include a history of extreme weather disruptions in the recent past resulting in an initially strong storage position; long−lived responses to historical and future prices; and expectations about the price of oil and effects of summer weather. The expected continued strength in future gas prices may be due to the

increasing demand for natural gas in electric generation. Edison Electric Institute's data shows that U.S. generation over the year in 2005 was often higher than in the previous five years. Another summer of strong electric demand growth for natural gas may be a factor in current futures prices, and this relationship between electric and gas markets is becoming increasingly important. Additions to U.S. generation capacity in 2005 totaled approximately 17 GW, down 25 percent from the prior year and down 75 percent from 2002. Additions in 2006 are likely to be roughly half the 2005 level. Gas is and likely will continue to be a dominant fuel for new generation for some time.
Report: http://www.ferc.gov/legal/staff−reports/eng−mkt−con.pdf
Source: http://www.ferc.gov/

2. *February 16, Chicago Tribune (IL)* — **More leaks at nuclear sites; Exelon discloses two additional tritium spills.** Radioactive tritium leaks have been found at two more nuclear power plant sites, Exelon Nuclear announced Wednesday, February 15, only weeks after the company disclosed a series of spills at a Will County plant. The leaks were discovered recently at Dresden Generating Station in Grundy County and Byron Nuclear Generating Station, about 25 miles southwest of Rockford, IL. So far, no tritium has been detected in groundwater off Exelon property near those plants, and the leaks "pose no health or safety threat," Exelon stated. The disclosures come weeks after Exelon publicly revealed water containing tritium spilled four times between 1996 and 2003 from vacuum breakers on an underground pipe at Braidwood Generating Station. Exelon detected groundwater tritium above levels permitted by the U.S. Environmental Protection Agency at two spots outside the plant. Tritium in one well was well above the normal "background" level. Exposure can increase the risk of cancer, birth defects and genetic damage. The leak at Dresden is the second discovered there in recent years. On Monday, February 13, a monitoring well showed tritium at levels 34 times higher than the federal limit, according to a Nuclear Regulatory Commission document.
Source: http://www.chicagotribune.com/news/local/chi−0602160265feb16,1,675760.story?track=rss

3. *February 15, NBC−2 (FL)* — **Worker killed at Fort Myers power plant.** A worker was killed at the Florida Power & Light (FP&L) plant on Palm Beach Boulevard Tuesday afternoon, February 14. FP&L spokesperson Grover Whidden says two men from West Palm Beach, FL, were inspecting the cooling towers when an external staircase collapsed. The men fell four stories to the ground. Whidden says Andres Sanderson died in the accident. Mark Diamond was treated for his injuries and released from the hospital. Federal investigators from the Occupational Safety and Health Administration and an FP&L safety team will investigate. Whidden says FP&L plants across the state are closing all external staircases until they can be inspected.
Source: http://www.nbc−2.com/articles/readarticle.asp?articleid=5860 &z=3&p=

[Return to top]

## Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

# Defense Industrial Base Sector

4. *February 16, Aviation Week* — **Revamped TSAT following new approach to risk, Sega says.** The newly restructured Transformational Satellite (TSAT) program is the first major effort to follow the Air Force's new approach to distributing risk in its space acquisition programs, according to Air Force Under Secretary Ronald Sega. To avoid the schedule slips and multibillion−dollar cost overruns that have plagued space programs like the Space Based Infrared System and National Polar−orbiting Operational Environmental Satellite System, the Air Force is trying to make sure enabling technologies are more mature before programs enter their later, costlier production phases. "We are going in with more mature technologies, with more stable requirements, with more discipline in the systems design," Sega told reporters during a press roundtable at the Pentagon Tuesday, February 14. "And the expectation is that the cycle time will be reduced and we'll be able, with higher confidence, to maintain cost and schedule." However, this is not necessarily a "risk−averse" approach, Sega said. The Air Force actually is encouraging more risk in earlier phases of program development.
Source: http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?id=news/TSAT02166.xml

5. *February 16, Defense News* — **U.S. Army seeks urban technology.** Densely populated urban areas require technology suited for them, said Maj. Gen. Roger Nadeau, who heads the U.S. Army's research and development command. Nadeau said too many weapons are being developed to fight on wide−open battlefields that bear little resemblance to the likely fields of conflict in an increasingly urbanized world. The Army will invest only in technologies that help its soldiers where they actually confront the enemy. He challenged industry to come up with new and more innovative ways of thinking. Nadeau said the service needs to rethink its multibillion−dollar Future Combat Systems program and the entire concept of network−centric warfare, and should ask whether the new technologies will really improve a soldier's ability to fight in an urban environment. According to Nadeau, what is needed is: better night−vision devices for soldiers and vehicles, sensors to allow troops to see through walls and buildings, active protection systems for vehicles that work in short−range urban environments, and even an improved bunker−busting type weapon to allow soldiers to breach walls.
Source: http://www.defensenews.com/story.php?F=1539002&C=america

6. *February 15, Air Force Link* — **Air Force regains decision authority on acquisition programs.** The Air Force recently regained oversight authority on some of the acquisition programs taken from it more than 10 months ago. The Department of Defense (DoD) returned major milestone decision authority to the Air Force on 10 of 21 acquisition programs in January. The DoD had taken that authority from the Air Force in March, amid concerns over a service leadership void and Air Force acquisition practices. At the time program oversight was transferred to the office of the secretary of defense (OSD), the Air Force had no confirmed secretary, undersecretary or assistant secretary for acquisition. The service had also experienced issues on Capitol Hill over some of its acquisition practices, said Lt. Gen. Donald Hoffman, Air Force military deputy for acquisition. While the Air Force still has no civilian assistant secretary for acquisition, the service does now have a confirmed secretary and undersecretary. The Air Force has also made strides in acquisition transparency, General Hoffman said. Among the 10 programs that were returned to the Air Force are the Joint Primary Aircraft Training System; the C−130 Aircraft Avionics Modernization Program; the Advanced Medium Range

Air−to−Air Missile; and the C−5 Aircraft Reliability Enhancement and Re−engining Program.
Source: http://www.af.mil/news/story.asp?id=123016340

7. *February 15, Defense News* — **U.S. Army leaders outline 2007 Budget needs.** The U.S. Army is rebalancing its fighting force, dedicating more troops to Iraq while modernizing its capabilities for the 21st Century, its top leaders said Tuesday, February 14. Army Secretary Francis Harvey and Army Chief of Staff Gen. Peter Schoomaker testified for two hours in front of the Senate Armed Services Committee during a hearing on the Army's fiscal 2007 budget request. They answered questions on body armor, the Future Combat Systems (FCS) program, pay for wounded soldiers, Army National Guard and Reserve end strength, recruiting challenges and funding the replacement of equipment destroyed in combat. Harvey emphasized the importance of fully funding the FCS program. "This is the key modernization program for the Army," he said. "It's really the first major modernization effort in four decades." The first spin−out of FCS technology is expected in 2008, with the introduction of unattended ground sensors, non line−of−sight launch systems and the intelligent munitions system, Harvey said. The Army also is working to up−armor its Humvees. "The reality is this," Schoomaker told the Senators. "We started the war with less than 500 up−armored Humvees. Now we're up−armoring everything, and we're going to continue anticipating and producing."
Source: http://www.defensenews.com/story.php?F=1537005&C=america

[Return to top]

## Banking and Finance Sector

8. *February 16, Silicon.com* — **Scammers ready with a scam for everyone; Pyramid schemes, lotteries, or phishing.** Younger, more affluent consumers are just as likely as vulnerable, older consumers to be targeted by scammers. Research from the Office of Fair Trading (OFT) shows that nearly half of the UK population −− or 20 million consumers over the age of 15 −− have been targeted by a scam. Pyramid schemes, lotteries, phishing or 419 scams are often spread through Websites and e−mails. The OFT said people most likely to be targeted by scammers are in the middle age ranges, with 54 percent of people between 35− and 44−years−old and 58 percent of people between 45− and 54−years−old having been targeted by a mass−marketed scam in the last two to three years. Working people were more likely to have been targeted than those who were not working. And nearly one in ten of those targeted had actually fallen victim to the scammer and parted with money. According to the OFT, the results run counter to expectations that the main focus for scammers would be the most obviously vulnerable consumer groups −− older people, or those isolated from social networks such as the workplace.
Source: http://software.silicon.com/security/0,39024655,39156510,00. htm

9. *February 16, VNUNet* — **Industry struggles to tackle phishing.** The latest development is the rise of corporate phishing, where attackers aim to steal confidential information or gain access to corporate networks. Attackers often use instant messaging to contact their victims, as many businesses use such networks internally. And few spam filters will catch an e−mail sent from a domain that is made to look like that of a bank. The panelists stated that financial institutions are failing to use best security practices; many fail to encrypt all the pages on their corporate Websites, which causes users to stop looking for the padlock indicating that a site is using

encryption. They may use confusing domain names, which creates complacency when users reach a site with an awkward domain name. Some phishing e−mails are sent at a rate of one million every four hours. The average phishing Website stays online for eight hours, and catches 15 to 20 victims for every million e−mails sent. Phishers have shown increasing sophistication recently, using cross site scripting, which eavesdrops on communications with a legitimate service, or bogus Websites that appear legitimate through the use of security certificates. But most phishers will not bother setting up such elaborate schemes, said Tod Beardsley of Tipping Point.
Source: http://www.vnunet.com/articles/print/2150403

**10.** *February 16, Newsday (NY)* — **Man sentenced in reservist ID theft.** A former janitor at Fort Totten in Bayside, NY, was sentenced Wednesday, February 15, to 18 months to three years in prison for stealing the identity of an Army reservist deployed in Kuwait and using a Neiman Marcus credit card to buy $3,000 worth of clothes. Authorities say Edwin Gomez, 35, had schemed to use the personal identities of more than 150 Army reservists, including many deployed to the Middle East. Gomez had an unauthorized credit card in a reservist's name and 15 pages of personnel lists and other military documents containing the reservists' names, ranks, and serial numbers when arrested, officials said. Queens District Attorney Richard Brown said, "Fortunately, the monetary damage was minimal as the defendant was apparently just getting started using the stolen reservists' identities." Authorities began investigating after a reservist returned to Staten Island from a duty tour in Kuwait and discovered unauthorized credit card charges on his credit report. Gomez pleaded guilty to second−degree identity theft and admitted opening a Neiman Marcus credit card in the reservist's name and purchasing goods via Internet. Gomez worked about three days between September 1 and November 14, as part of the janitorial staff at Fort Totten.
Source: http://www.stamfordadvocate.com/news/local/newyork/nyc−nysen t164628848feb16,0,6677867.story

**11.** *February 15, Computeractive* — **BT publishes guide to help prevent online identity theft.** BT, a UK communications solutions provider, has released a ten−point guide to help prevent Internet users falling victim to online fraud and identity theft. The guide forms part of an Internet security report highlighting growing and future online threats, published in conjunction with Yahoo, the UK government's Get Safe Online campaign, and the Metropolitan Police. The report found that 62 percent of consumers surveyed thought that online fraud could not happen to them. Over 40 percent said that they were not aware whether they had been victims of online fraud or not. Although only eight percent of those surveyed have been victims of online fraud in the last year, the problem is growing because consumers are unaware of the major new and rapidly growing threat of online identity theft. Consumers seem unaware that the Internet and not their trashcan is the place criminals are now most likely to use to steal personal information. Detective Chief Superintendent Nigel Mawer said, "Online identity theft and fraud are the latest techniques." The report gives consumers a comprehensive overview of new and emerging online threats and a comprehensive list of where people can go to report cybercrimes.
Report: http://www.btplc.com/onlineidtheft/onlineidtheft.pdf
Source: http://www.computeractive.co.uk/computeractive/news/2150336/bt−publishes−guide−prevent

**12.**

*February 15, SecurityPark* — **Websense Security Labs launches Global Phishing and Crimeware Threat Map and security blog.** Websense, Inc.'s interactive Global Phishing and Crimeware Threat Map displays the most recent data collected by Websense Security Labs and provides a historical look into where phishing and crimeware related Websites are hosted on the Internet. Upon discovery, each site is looked up via its IP address to track the country of origin through the appropriate IP registrars and plotted on the map. The map shows the location of phishing and crimeware sites on an interactive map of the world. The data is updated by Websense Security Labs approximately 15 minutes after discovery. Threats around the globe can be searched by geographic region, date, and threat types. Over the past few months, Websense Security Labs has seen a major increase in the number of phishing and crimeware related Websites in the Republic of Korea and China. The U.S. continues to be the top country of origin for Internet criminal activity. Websense Security Labs has also begun publishing a security blog. "In less than a year's time, we have seen phishing techniques evolve from what would appear to be done for bragging rights between hackers to what is now full fledged electronic crime," said Dan Hubbard of Websense.
Source: http://www.securitypark.co.uk/article.asp?articleid=24964&Ca tegoryID=1

13. *February 14, U.S. Department of Justice* — **Texas man pleads guilty to filing false claim with FEMA for Katrina disaster funds.** On Tuesday, February 14, Clifford Neville, 53, of Houston, TX, was convicted of filing a false claim with the Federal Emergency Management Agency (FEMA) for Hurricane Katrina Disaster funds. At sentencing, Neville faces a maximum punishment of five years imprisonment and a $250,000 fine. The case against Neville is the result of an investigation initiated by a tip to the U.S. Department of Homeland Security's Office of Inspector General (DHS−OIG). According to the tip, Neville had filed a false claim for FEMA assistance. DHS−OIG agents found that two claims had been filed in Neville's name for FEMA Hurricane Katrina disaster assistance. The first claim, filed on September 9, 2005, listed Neville's primary residence in New Orleans. Based on that claim, Neville received $2,000 in expedited disaster assistance. Further investigation by DHS−OIG agents proved not only that Neville had been living in Houston when Hurricane Katrina struck New Orleans, but that Neville had never resided in New Orleans. On October 1, 2005, the second claim was filed for disaster assistance. The second claim again listed the primary residence in New Orleans. Because the information in the second claim matched the information from the first, FEMA computers flagged the second claim.
Source: http://www.usdoj.gov/katrina/Katrina_Fraud/HKFTF_PressRoom/2 −14−06USAOSDTX.pdf

[Return to top]

## Transportation and Border Security Sector

14. *February 16, Reuters* — **El Al fits fleet with anti−missile system.** El Al Israel Airlines has installed anti−missile systems on all its planes, becoming the first commercial carrier to field a protected fleet amid growing fears of aviation terrorism, security sources said on Wednesday, February 15. They said aircraft were equipped with the Israeli−made "Flight Guard" which automatically releases diversionary flares if a heat−seeking missile is detected by on−board sensors. Development of the system, which costs around $1 million per unit, was stepped up after an Israeli passenger jet survived an attempt by al Qaeda to shoot it down over Kenya in

2002. Industry analysts say fitting military equipment to civilian planes would pose cost problems for many airlines, since such systems must be constantly serviced. The likelihood of a shoulder−fired missile actually downing a passenger jet is considered to be remote, as such aircraft are built to withstand the loss of an engine. Though Flight Guard would be effective against heat−seeking missiles like the SA−7, produced in the former Soviet Union and widely available in the developing world, it would not be effective against radar−guided missiles.
Source: http://www.usatoday.com/travel/flights/2006−02−16−anti−missile−airline−system_x.htm

15. *February 16, Associated Press* — **Nevada airport officials demand answers after equipment fails.** Officials at Reno−Tahoe International Airport demanded answers Wednesday, February 15, after new, high−tech equipment designed to keep the airport open in poor weather failed, causing five flight diversions and a ripple of delays. "This is completely and absolutely unacceptable," said airport spokesperson Brian Kulpin. A spokesperson for the Federal Aviation Administration (FAA) in Seattle confirmed that the Mark 20A instrument landing system went down around 5:40 p.m. Tuesday, February 14. The system is operated and maintained by the FAA. "We got people in there almost right away," said FAA spokesperson Allen Kenitzer. "They're trouble shooting it, trying to figure out the problem. Kulpin said FAA officials indicated there had been "some type of wiring issue" that caused the malfunction. The $2 million equipment at the Reno airport was installed last year and unveiled just before the Thanksgiving Day holiday travel rush. It replaced older equipment that had failed five times in the previous four years. Two of those failures occurred in November 2004, stranding thousands of passengers and causing the delay or cancellation of 154 flights.
Source: http://www.usatoday.com/travel/flights/2006−02−16−reno−airpo rt−equipment_x.htm

16. *February 16, Newsday (NY)* — **Increasing ridership on the LIRR.** Reversing a downward trend, the Long Island Rail Road (LIRR) saw ridership rebound in 2005, the first year of growth since 2001, with increases in monthly and weekly ticket sales, according to railroad officials. About 80.2 million passengers took the trains in 2005, and many riders said they are more satisfied with the job the railroad is doing, according to the 2005 LIRR Customer Satisfaction Study, released on Wednesday, February 15. Experts say job gains in the industries where many riders are employed, such as the financial, real estate, and insurance sectors, contributed to the increase. Brian Dolan, a spokesperson for the LIRR, said rising gasoline prices also had an impact on ridership, as did the transit strike at the end of December, when the railroad sold an extra 351,000 tickets. The Long Island Rail Road is the busiest railroad in North America. Stretching from the eastern tip of Montauk, Long Island to Penn Station in Manhattan.
Source: http://www.newsday.com/news/local/longisland/ny−lilirr164628798feb16,0,821000.story?coll=ny−top−headlines

17. *February 16, Reuters* — **New York bus station reopens after suspect package.** New York city's biggest bus terminal was briefly evacuated during lunchtime on Thursday, February 16, as police inspected a suspicious package, but the station was opened shortly after, police on the scene said. Police at the Port Authority said the problem had been cleared up and people were being allowed to re−enter the transportation hub on 42nd Street.
Source: http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006−02−16T182508Z_01_N16372788_RTRUKOC_0_US−SECURITY−NEWYORK.xml

18. *February 16, Business Journal (AZ)* — **Arizona governor extends state of emergency at Mexican border.** Governor Janet Napolitano has extended a state of emergency order at the Mexican border allowing local government more time to spend $1.5 million in state emergency funds on law enforcement and other immigration matters. Napolitano issued a state of emergency for Arizona counties bordering Mexico last August. Her new move extends that emergency until August 2006 and gives local governments more time to allocate state money. Arizona has become a top entry point for illegal immigrants and drug trafficking from Mexico that is straining state and local police and prisons. The governor also has put forward a $100 million immigration and border security package in her budget and favors state fines against employers who hire illegals as well as a guest worker program. Napolitano's border emergency declaration last year coincides with a similar move by New Mexico Governor Bill Richardson.
Source: http://phoenix.bizjournals.com/phoenix/stories/2006/02/13/da ily43.html

[Return to top]

## Postal and Shipping Sector

19. *February 16, Reuters* — **Global air cargo investigation reaches Asia.** A global probe into possible price fixing in the air cargo industry widened to Asia on Wednesday, February 15, as authorities searched for information at offices of Japanese, South Korean, and Hong Kong airlines. The investigation started Tuesday, February 14, when the European Union's executive arm and the U.S. Department of Justice raided a number of air cargo carriers on both sides of the Atlantic, while other airlines were asked for information related to the probe. The case could threaten to halt recent growth in the $50 billion global air cargo market. The cargo business accounts for some 12 percent of revenue in the global commercial aviation market, according to the International Air Transport Association. The European Commission said in a statement, "The Commission has reason to believe that the companies concerned may have violated (a European Union) treaty, which prohibits practices such as price fixing." It declined to name the targets. Among airlines, Korean Air is the world's top cargo carrier, based on 2004 data, although it ranks behind specialist carrier FedEx Corp. in total volume flown.
Source: http://money.cnn.com/2006/02/15/news/international/air_cargo .reut/index.htm?cnn=yes

20. *February 15, North Platte Telegraph (NE)* — **False alarm at Nebraska mail center.** A mysterious yellow/white power found in a mail crate Tuesday night, February 14, which temporarily closed the North Platte, NE, mail−processing center, may be fire extinguisher residue. Tests on the scene Tuesday, when the powder was reported, ruled out anthrax. Employees who came in contact with the substance were isolated and all employees were moved into a safe zone until the substance could be identified. Fire crews and an ambulance responded to a call from employees at the center at 7:38 p.m. CST Tuesday. North Platte police set up a perimeter. Emergency responders treated the scene as a worst−case scenario, said battalion chief Chris Jarvis. Members of the State Emergency Response Team were called to the scene. North Platte Postmaster Daniel Becker said the episode caused some delay in processing the mail. "The post office was down for about six hours," Becker said. "The percentage of mail affected is very small."
Source: http://www.nptelegraph.com/site/news.cfm?newsid=16134937&BRD

=377&PAG=461&dept_id=531813&rfi=6

[Return to top]

## Agriculture Sector

**21.** *February 16, Medford News (OR)* — **Research center will allow scientists to pursue new avenues of fish study.** Steelhead are spawning in the new artificial stream channels at the Oregon Hatchery Research Center in the Alsea River basin, and researchers have begun studying how the fish choose mates and where they prefer to spawn −− key factors in preserving fish runs. But it is the future of scientific inquiry that has fish researchers excited about this new facility, which is jointly operated by the Oregon Department of Fish and Wildlife and Oregon State University's Department of Fisheries and Wildlife. Fish have a bony structure within their ears called an otolith, which accretes calcium carbonate. By examining the isotopes within the otolith, they can amass critical new data about the age of fish, where they have lived and what they have eaten, said David Noakes, a professor of fisheries at the Oregon Hatchery Research Center. "These otoliths are like flight recorders," Noakes said. These isotopic signatures may eventually be refined enough to pinpoint how long fish have been in freshwater, at what depth in the ocean they swam, and what types of prey they ate while at sea −− all critical to gaining a better understanding for how to protect different species.
Source: http://www.medfordnews.com/articles/index.cfm?artOID=327668& cp=10996

**22.** *February 16, Agence France−Presse* — **Croatia says one cow tested positive for mad cow disease.** Croatia's veterinary institute said first tests had shown one cow in the east of the country to have contracted mad cow disease, national television reported. The tests "confirmed that the five−year−old cow had mad cow disease," the television said, adding that the samples will be also sent to a laboratory in Britain. It is the first reported mad cow case in the Balkans country. The cow which was slaughtered at a farm in eastern Croatia was not previously showing symptoms of the disease, which was confirmed in regular tests conducted for all slaughtered cattle over 30−month−old. It was calved in Croatia, but its parents were imported from Austria, the television added.
Source: http://news.yahoo.com/s/afp/20060216/hl_afp/croatiahealthmadcow_060216191608;_ylt=AkVD5Rz_vSDjUab5PqXmX.iJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

**23.** *February 14, CBC News (Canada)* — **Record year for chronic wasting disease.** Thirty−six wild deer have tested positive for chronic wasting disease (CWD) in Saskatchewan, Canada, this year −− the highest number ever recorded in one year since the province started testing for the degenerative nerve disease. The 36 are mostly mule deer and come from just about every region of the province. Of those, 32 were taken by hunters while the other four were either found dead in the woods or were obviously sick. Three of the infected deer came around Love, south of Nipawin, and all three are said to have fed at the same bait station set out by hunters to attract animals. Jurisdictions around North America have banned deer baiting or are encouraging hunters not to bait or feed deer. Manitoba, where there is a ban, hasn't had a confirmed case of CWD in wild deer. The argument against baiting is that it concentrates deer and increases the likelihood of spreading disease in a deer herd. But while some see the link between deer baiting and CWD as conclusive, the official Saskatchewan government response

is that there is still no clear connection.
CWD information: http://www.cwd−info.org/
Source: http://www.cbc.ca/sask/story/deer−cwd060214.html

[Return to top]

## Food Sector

**24.** *February 16, Agricultural Research Service* — **Tiny animals aid salmonella.** Salmonella, one of the planet's most problematic food−poisoning bacteria, may have an accidental ally: transparent, nearly invisible animals called protozoa. Agricultural Research Service microbiologist Maria Brandl has provided new evidence of the mostly mysterious interaction between these microscopic protozoa and Salmonella. Brandl's discoveries may lead to new, more powerful, and more environmentally friendly ways to reduce the incidence of Salmonella in meat, poultry, and fresh produce. During their lives, Salmonella bacteria may encounter a commonplace, water−loving protozoan known as a Tetrahymena. Brandl's laboratory tests showed that the protozoan, after gulping down a species of Salmonella known as S. enterica, apparently can't digest and destroy it. So, the Tetrahymena expels the Salmonella, encased in miniature pouches called food vacuoles. The encounter may enhance Salmonella's later survival. Brandl found that twice as many Salmonella cells stayed alive in water if they were encased in expelled vacuoles than if they were not encased. What's more, Brandl found that the encased Salmonella cells were three times more likely than unenclosed cells to survive exposure to a 10−minute bath of two parts per million of calcium hypochlorite, the bleach−like compound often used to sanitize food and food−processing equipment.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

**25.** *February 16, Associated Press* — **Man arrested for tampering with baby formula.** Federal prosecutors say a man has been charged with replacing powdered infant formula with flour and salt before returning the container to a store, where it was repurchased and sickened a child in Cecil, MD. Bobby Wayne Rhoades, was arrested Tuesday, February 14, and charged with tampering with consumer products. Prosecutors say a review of security videotapes where the formula was purchased led police to Rhoades. Prosecutors say the child's parents discovered a hole in the container covered by tape after their child became ill and the label fell off the container. The contents of the container were later analyzed by the U.S. Food and Drug Administration forensic chemistry center, which determined it held flour and salt instead of formula.
Source: http://wjz.com/health/local_story_047104051.html

**26.** *February 16, USAgNet* — **Taiwan welcomes back U.S. beef.** Shipments of U.S. beef started arriving in Taiwan last week −− which were the first to arrive since June, when Taiwan banned U.S. beef after the announcement of a second case of bovine spongiform encephalopathy (BSE) in the U.S. American beef products will be available in retail markets this week, and a survey by the Department of Health in Taiwan indicates 65 percent of Taiwanese consumers will buy U.S. beef. Carrefour, operating 37 outlets in Taiwan, will also conduct a media event to reintroduce U.S. beef to customers. Many wholesale stores, steakhouses, and hot−pot restaurants in Taiwan have reported increased inquiries from customers who favor the special flavors of U.S. beef. Taiwan initially banned U.S. beef in December 2003 after the U.S.

discovered its first case of BSE. At that time, Taiwan was on the list of top 10 export markets for U.S. beef and beef variety meat with 19,225 metric tons valued at $76.5 million going to Taiwan.
Source: http://www.usagnet.com/story−national.cfm?Id=181&yr=2006

**27.** *February 16, Japan Economic Newswire* — **U.S. disqualifies plant as processor of beef for shipment to Japan.** The U.S. government has informed Japan that it has disqualified major U.S. meat packer Swift Beef Co.'s plant in Nebraska as a processor of beef for export to Japan due to a violation of procedures, the Japanese government said Thursday, February 16. The Nebraska plant is one of the 38 slaughterhouses authorized to process beef for shipments to Japan. According to the information from Washington, Swift Beef has presented the U.S. Department of Agriculture with a quality control program stating that its head office would designate suppliers of cattle whose ages can be confirmed in compliance with conditions set by the Japanese government, said the Ministry of Health, Labor and Welfare and the Ministry of Agriculture, Forestry and Fisheries. It turned out, however, that the Nebraska plant made the designation on its own, the ministries said. In mid−December, Japan lifted a two−year−old ban on U.S. beef imports it imposed due to mad cow disease concerns. The Japanese government reintroduced the ban on January 20 after a prohibited backbone was found in a shipment of beef from the U.S. The procedural violation by the Nebraska plant was found through a U.S. government investigation conducted under terms agreed upon for the resumption of American beef imports.
Source: http://www.tmcnet.com/usubmit/2006/02/16/1379608.htm

[Return to top]

## Water Sector

**28.** *February 15, Xinhua (China)* — **Africans lack drinking water.** One−third of the African population have no drinking water and almost half of the African people have health problems due to the lack of clean drinking water, a report said on Tuesday, February 14. If the current situation can't be improved, at least 17 African countries will suffer from a severe water shortage by 2010, said a report released at the 13th Congress of the African Water Association (AFWA) in the Algeria capital of Algiers. The water shortage will also lead to clashes between some countries in the region, the report warned. Africa has abundant water resources amounting to 5.4 trillion cubic meters, but only four percent of them have been developed and utilized because of the lack of funds and facilities. The four−day AFWA meeting drew the attendance of more than 400 representatives from over 30 African countries.
Source: http://news.xinhuanet.com/english/2006−02/15/content_4183654 .htm

**29.** *February 14, Express−Times (NJ)* — **Security risk of water system under scrutiny.** Pennsylvania State Police are surveying the security of the water system serving Bethlehem and 10 neighboring municipalities. "We will offer some recommendations, if necessary, to enhance the security of their water system," said Trooper Chris Bayzick, from the department's Office of Domestic Security Risk and Vulnerability Assessment Team. He said the survey should take a few weeks. The city water authority Thursday, February 16. It began with a preliminary fly−over of the 39−square−mile watershed in Carbon and Monroe counties from where the water flows, according to Bethlehem Authority Executive Director Stephen Salvesen. State

police conduct these free surveys for anyone who asks, Bayzick said. "They'll have a good idea what the scope and breadth of the system is," Salvesen said of the state police. "They'll be in the loop if something does happen to the system." The watershed is patrolled by one authority police officer. Previous incidents there have included tree thefts, ATV riding, and hunting in restricted areas.
Source: http://www.nj.com/news/expresstimes/pa/index.ssf?/base/news-4/113989383613180.xml&coll=2

30. *February 14, Knight Ridder Newspapers* — **Lack of safe drinking water is a daily problem in China.** As China gallops toward the modern era, access to safe and clean drinking water is beyond the reach of hundreds of millions of rural and urban people. Chemical spills, rampant pollution, and poor stewardship of the land have tainted much of the nation's water supply, and the ground water under 90 percent of China's cities is contaminated The World Health Organization (WHO) says 700 million of China's 1.3 billion people drink water that doesn't meet WHO's minimum standards, primarily due to improper treatment of industrial, human and animal waste. Barely 20 percent of China's sewage is adequately treated. China's vice minister of water resources, E Jingping, said on December 28, 2005 that some 300 million rural residents drink water contaminated by fluorine, arsenic, high levels of salt, or other organic or industrial pollutants. At least five major toxic spills and dozens of minor ones have sloshed into rivers in China in the past three months and made it into Chinese news reports. Well-off residents of cities can buy bottled water, but impoverished Chinese have no choice but to drink tap or well water. They always boil it, which can kill bacteria and parasites but won't remove chemical contaminants.
Source: http://www.mercurynews.com/mld/mercurynews/news/world/138707 30.htm

[Return to top]

## Public Health Sector

31. *February 16, Deutsche Presse-Agentur* — **European Union adopts tough new anti-bird flu measures for poultry.** European Union veterinary experts Thursday, February 16, agreed on tough new measures to prevent outbreaks of bird flu in poultry farms across the bloc following earlier precautionary action taken against infected wild birds. Commission officials said the bloc's governments were on full alert and working on the assumption that there was a high risk more bird flu cases would be found across the bloc. Under the new measures, any cases of bird flu in poultry farms must be followed up immediately by the establishment of a huge buffer zone to prevent further spread of the disease to other parts of the country. Officials said poultry farms in this area would be subject to very strict controls and birds would have to be kept inside. The buffer zone could be very large and could cover a "department, a province or even an entire region," the officials added. Such a high risk area will be in addition to a two mile wide protection zone within which infected birds will have to be culled and movement of poultry will be banned except when birds are en route to a slaughterhouse.
Source: http://news.monstersandcritics.com/health/article_1130552.php/EU_adopts_tough_new_anti-bird_flu_measures_for_poultry

32. *February 15, Agence France-Presse* — **Toll from mosquito-borne epidemic in Reunion island nears 100,000.** The toll in the Indian Ocean island of Reunion from a mosquito-borne

virus that causes crippling pain in the joints is likely to reach 100,000 by week's end, the minister for France's overseas territories, Francois Baroin, said. "We will probably reach the figure of 100,000 cases of chikungunya in Reunion by the end of the week," he said. Baroin added that the tally of cases in the island of Mayotte, a French overseas territory in the Comoros Indian Ocean archipelago, was expected to rise to more than 500. Reunion, a French department with a population of 776,000, first detected chikungunya in March 2005. The president of France's Institute for Development Research (IRD), Jean−Francois Girard, on Monday, February 13, said it was biggest epidemic of chikungunya ever recorded anywhere. Chikungunya is caused by a virus spread by mosquito. It is not known to be fatal but can cause painful swelling of joints in the body, leaving victims stooped and limiting their movements. There is no vaccine.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://news.yahoo.com/s/afp/20060215/hl_afp/francereunionhealth_060215183909;_ylt=AizkTSs3Zen4loDsqNvPIrGJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

**33.** *February 15, Associated Press* — **Europe going on guard against bird flu.** European governments are bolstering their guard against bird flu. France, Germany, the Czech Republic, Switzerland, and Sweden all took steps Wednesday, February 15, to try to prevent the spread of the H5N1 strain, ordering that domestic fowl be kept in screened, ventilated buildings. Britain and the Netherlands ordered similar precautions. The fear of birds migrating from Africa has been augmented by the deaths of swans from the Baltic Sea to the southern tip of Italy. The first swan deaths in Europe were recorded in Croatia in October, leading to controls on contacts with wild birds. In Austria, authorities said two swans found dead were infected with H5N1. At least nine dead swans have been found on Danish islands in the Baltic, and two swans died in Germany. In Slovenia, a swan infected with bird flu was found dead last week. Laboratory tests are still under way to determine whether it is the H5N1 strain. Bulgaria has confirmed one swan death from H5N1 and is testing three others. Greece has four confirmed cases in three swans and a goose and Cyprus has a confirmed case in a chicken. Italy confirmed six swans died of the disease.
Source: http://abcnews.go.com/Health/wireStory?id=1623415

**34.** *February 15, Agence France−Presse* — **U.S. mobilizes global effort against bird flu.** The U.S. has stepped up its global efforts to contain the spread of bird flu. While the avian disease hasn't been detected inside the U.S., "We are not exempt," said Kent Hill, assistant administrator for global health at the U.S. Agency for International Development. The U.S. Centers for Disease Control and Prevention (CDC) sent a team of medical and veterinary specialists this week to Nigeria to help halt a new outbreak in the country's north. The CDC has also recently sent epidemiologists and laboratory technicians to Kenya, said spokesperson Kathy Haerben. But even as it tries to stall bird flu's spread, Washington is also monitoring the possibility that the organism's mutation could enable it to jump easily from fowl to human and then from one person to another. "The challenge is to limit as much as possible how much contact there is between infected birds and people, and just to limit the extent of the spread among the birds," Hill said. "(We) work with World Health Organization and in places where H5N1 is not even identified ... We are working with the countries to make sure they are anticipating what they do if they get an outbreak," said Hill.
Source: http://news.yahoo.com/s/afp/20060215/hl_afp/healthfluus_0602

15172512;_ylt=Andaybb46XaihNeUW0baG06JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

## Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

**35.** *February 16, Arizona Republic* — **Thousands in potential disaster drill.** Arizona's Coyote Crisis Campaign is planning a large−scale homeland security drill which will test the ability of civilian and military authorities to function together in an extreme emergency with more than 10,000 casualties. The chief participants, Arizona's Army and Air National Guard, General Dynamics, Scottsdale and Scottsdale Healthcare, started meeting a year ago to plan for a regional response to terrorist attacks or natural disasters. Despite orange terrorism alerts since the September 11 attacks, no broad disaster plan had arisen involving government, military, academic institutions and private industry, according to Coyote Crisis Campaign leaders who intend for their project to become a model for other regions. The Coyote project is based on military opinion that a terrorist attack will happen and the recognition by area civil and health authorities that they may not be prepared for it, leaders say. The disaster drill, to be held April 25−28, includes both live and simulated events and involves Luke Air Force Base, Arizona State University, Maricopa County and major utilities. Organizers expect to involve 3,000 individuals in the drill.
Source: http://www.azcentral.com/arizonarepublic/local/articles/0216 disaster0216.html

**36.** *February 15, National Journal's Technology Daily* — **First responders detail emergency communications problems.** House lawmakers and emergency responders on Wednesday, February 15, agreed that more needs to be done to establish emergency communications systems that function across jurisdictions. A lack of equipment standards, inadequate funding and turf wars among federal, state and local officials have made it increasingly difficult to achieve interoperable emergency communications, a panel of first responders said at a House Homeland Security Emergency Preparedness, Science and Technology Subcommittee hearing. Wisconsin State Patrol Chairman Casey Perry attributed a great deal of his problems to squabbles among states, counties and municipalities. He said more federal grant money needs to be conditional to hold state and local governments accountable for creating interoperable networks. "Each entity resists losing their share of control," Perry said. "This is the underlying root of the problems we face today." William Maroney, president of the United Telecom Council, said utilities need to be more included in the process because they can build infrastructures that help communications systems function during disasters. He urged the committee to invest judiciously in technology and said that throwing money at the latest devices would not solve the problem on its own.
Source: http://www.govexec.com/story_page.cfm?articleid=33406&dcn=to daysnews

37. *February 15, Government Computer News* — **HSPD−12 to get its first field test.** The Pentagon will host an exercise next week to demonstrate smart−card interoperability among federal, state and local emergency personnel in the Washington, DC−metro area. The Winter Fox exercise, scheduled for Thursday, February 23, would be the first field test of the First Responders Access Card, an initiative of the multigovernmental National Capital Region. The card is expected to meet technical specifications for the federally mandated Personal Identity Verification card. The First Responder Partnership Initiative includes agencies in Montgomery and Prince George's counties in Maryland; Arlington, Fairfax and Prince William counties in Virginia; as well as Washington and federal agencies including the Departments of Homeland Security, Defense, and Health and Human Services. The cards are intended to enable communication and access across jurisdictional boundaries during emergencies.
Source: http://www.gcn.com/vol1_no1/daily−updates/38272−1.html

38. *February 15, Deseret News (UT)* — **Utah test explosion is part of class on sifting evidence.** In an exercise conducted Tuesday, February 14, at the Utah Test and Training Range, two huge bombs blew up a van and ambulance. Each bomb was reportedly made from ammonium nitrate and diesel fuel, ignited by a blasting cap. The 44 students' objective in FBI special agent Kevin Miles' class was to sift through the debris aftermath, looking for evidence of what type of explosive device ripped apart both vehicles. Students in Miles' free class will, for example, find out what a D battery looks like after it's been in an explosion, according to Salt Lake, UT, FBI special agent Michael Brogan. "Every crime scene is different," he said. "Everything is there after an explosion −− it's just in real, real small pieces. You just have to know what to look for." About half of the students were military personnel, but the rest were from law enforcement agencies in Chicago, Michigan, Florida and Kentucky. Miles' class has a waiting list of about 500 −− 300 of whom are military.
Source: http://deseretnews.com/dn/view/0,1249,635184590,00.html

[Return to top]

## Information Technology and Telecommunications Sector

39. *February 15, FrSIRT* — **Nullsoft Winamp Playlist handling multiple buffer overflow vulnerabilities.** Multiple vulnerabilities have been identified in Winamp, which could be exploited by remote attackers to take complete control of the affected system. Analysis: The buffer overflow error when processing a specially crafted playlist containing an overly long media filename, which could be exploited by remote attackers to compromise a vulnerable system via a specially crafted playlist. The second issue is due to a buffer overflow error when processing a playlist (.m3u) with an overly long filename, which could be exploited by remote attackers to execute arbitrary commands and take complete control of an affected system via a specially crafted Webpage. Affected products: Nullsoft Winamp version 5.13 and prior. Solution: FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2006/0613

40. *February 15, Tech Web* — **Homeland Security spells out coming online threats.** The top Internet threats for 2006 will include more attacks through instant messages and cell phones, as well as a boost in identity hacks against online brokerage accounts, the Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA) predicted

Wednesday, February 15. By joining forces, DHS and NCSA hope to give consumers time to put additional protection in place on their PCs. Calling instant messaging networks "extremely vulnerable" and noting that cell phone malware is on the rise, the federal agency and the non−profit also predicted more "spear phishing," or targeted phishing attacks. Other threats to expect, include an increase in brokerage account break−ins.
Source: http://www.informationweek.com/news/showArticle.jhtml?articl eID=180202429

41. *February 15, Tech Web* — **Chertoff says IT weaknesses hurt Katrina response.** Department of Homeland Security Secretary Michael Chertoff took responsibility for the poor response to Hurricane Katrina Wednesday, February 15, but he also blamed the department's inability to conduct surveillance, communicate efficiently, track shipments, and handle Web traffic. Testifying before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Chertoff said the Department of Homeland Security and the Federal Emergency Management Agency need interoperability, hardened communications, a tracking system for shipments, improved surveillance resources, upgraded software and better hardware. Without hardened communications equipment, leaders could not obtain the information they need to make proper decisions during disasters, Chertoff said. Improvements are underway, but the department has to come up with agreements for supply chain management and real−time monitoring, Chertoff said.
Chertoff's remarks: http://www.dhs.gov/dhspublic/interapp/testimony/testimony_00 46.xml
Source: http://www.techweb.com/wire/security/180202527

42. *February 15, Windows IT Pro* — **Ten thousand dollar bug bounty offered.** iDefense announced that it will pay $10,000 to anyone who discovers a bug in a Microsoft product that results in a new Microsoft Security Bulletin with a severity rating of critical. But there's one slight catch: The bug must be reported by midnight March 31, 2006, EST. The company has paid for vulnerability reports for some time now. However iDefense is changing its tactics to some extent. A spokesperson for iDefense said, "Going forward, on a quarterly basis, we will select a new focus for the challenge and outline the rules for vulnerability discoveries that will qualify for the monetary rewards." iDefense competes against a growing underground market for vulnerability reports and exploit code, where reports and code are sometimes sold the highest bidder and other times sold to everyone who can pay the asking price.
Source: http://www.windowsitpro.com/windowspaulthurrott/Article/Arti cleID/49416/windowspaulthurrott_49416.html

43. *February 15, PC World* — **FBI director: Cyber threats fluid and far reaching.** Hacker hunters need to develop new techniques to take on the latest generation of sophisticated and well−organized cyber criminals, FBI Director Robert Mueller told attendees of the RSA Conference 2006 on Wednesday, February 15. In particular, Mueller said in a keynote address, the FBI must work with corporations and international law enforcement to help combat online criminal acts that are seldom reported. "Increasingly our cyber threats originate outside of the United States," he said. "The once−clear divisions of jurisdiction and responsibility between agencies [and nations]...have been rendered obsolete by the fluid and far−reaching nature of today's threats." The FBI now has more flexibility to work with international law enforcement and is helping build relationships with those foreign agencies by putting operatives "on the ground" in countries that may be hotbeds for cybercrime, according to Steven Martinez, the deputy assistant director for the FBI's Cyber Division, who spoke after Mueller.

Source: http://www.pcworld.com/news/article/0,aid,124741,00.asp#

### Internet Alert Dashboard

**DHS/US−CERT Watch Synopsis**

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US−CERT Operations Center Synopsis:** US−CERT is aware of publicly available exploit code for a memory corruption vulnerability in the Mozilla Firefox web browser and Thunderbird mail client. If JavaScript is enabled in these applications, then the system is vulnerable to exploitation. A vulnerable system may be successfully exploited if a user is convinced to visit a specially crafted web page or open a specially crafted email.

A remote, unauthenticated attacker may be able to execute arbitrary code on a compromised system. If the user has elevated privileges, then the attacker will be able to exploit them. For more information please review the following US−CERT Vulnerability Note:

VU#759273 − Mozilla QueryInterface memory corruption vulnerability at URL: http://www.kb.cert.org/vuls/id/759273

US−CERT urges users and administrators to implement the following recommendations:

See update to Firefox 1.5.0.1 at URL: http://www.mozilla.com/firefox/

Please see SeaMonkey 1.0. at URL: http://www.mozilla.org/projects/seamonkey/

Disable JavaScript in Thunderbird and Mozilla Suite.

**Current Port Attacks**

| | |
|---|---|
| **Top 10 Target Ports** | 1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft−ds), 18551 (−−−), 139 (netbios−ssn), 135 (epmap), 113 (auth), 32772 (sometimes−rpc7), 2234 (directplay)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

# Commercial Facilities/Real Estate, Monument &Icons Sector

**44.** *February 16, KHOU (TX)* — **Security increased for All−Star Weekend.** Houston will be all about basketball this weekend as thousands come to town for All−Star Weekend. And, police will be out in full force for the events. The Houston Police Department (HPD) and other law enforcement agencies have run security for the Super Bowl, the MLB All−Star Game, and the World Series. Metro police, the Texas Alcohol Beverage Commission and Public Works will also be out on the streets assisting HPD. They expect the event to be smaller than the Super Bowl but bigger than the World Series, and the situation will be different because they expect more celebrities.
Source: http://www.khou.com/news/local/houstonmetro/stories/khou0602169_ac_allstarsecurity.318e5ecd.html

[Return to top]

# General Sector

Nothing to report.
[Return to top]

**DHS Daily Open Source Infrastructure Report Contact Information**

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

**DHS Daily Open Source Infrastructure Report Contact Information**

| | |
|---|---|
| Content and Suggestions: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644. |
| Subscription and Distribution Information: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information. |

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.